Table of Contents

COMMONWEALTH OF MASSACHUSETTS
DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department of Telecommunications and Energy on its own Motion, Pursuant to G.L. c. 159, §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	**)**	**D.T.E. 02-8**

INITIAL BRIEF OF COVAD COMMUNICATIONS COMPANY

INTRODUCTION

In its *Vote and Order to Open Investigation* ("*Order*") dated January 24, 2002, the Department announced its desire to assess the adequacy of current security measures with respect to existing collocation arrangements in Massachusetts and, where they may be lacking, explore ways to make Verizon central offices more secure. The Department's effort to ensure a safe and reliable telecommunications infrastructure is both timely and warranted in the aftermath of the September 11th attacks. Covad Communications Company ("Covad") believes that this investigation, if properly focused, will result in a more secure telecommunications infrastructure as required by the public interest.

Through its participation in this proceeding, Covad has attempted to address the issues as raised by the Department, namely the current state of collocation security in Massachusetts. As discussed below, after months of pre-filed testimony, information requests and responses, pre-filed rebuttal testimony and three days of hearings, the evidence clearly shows that collocation security in Massachusetts is perfectly adequate, and that there is no relevant evidence showing that CLECs are any threat to security. The evidence does suggest strongly, however, that Verizon's own security practices could be enhanced, and that this can and should be done in a

manner that has no negative impact on the ability of CLECs to provide service in Massachusetts. Covad believes improving security in this manner should be an ongoing process, and we again encourage the Department to convene an industry task force to study and recommend best security practices in the industry for implementation in Massachusetts.

Verizon, unfortunately, has paid little attention to the Department's concerns in this proceeding. Unlike Covad's suggestions, which are a response to actual operating experience in Massachusetts COs, Verizon's proposals regarding new collocation security policies are not a response to any real, substantiated security threat, but rather just another thinly veiled attempt to re-litigate sound collocation rules and requirements in order to thwart competition in the market for facilities-based local services. Verizon suggests new rules in which CLECs would be allowed virtual collocation only in certain central offices, and separate space and entrances would be required for physical collocation arrangements in all others. These proposals (a) are not reasonably related to the minimization or elimination of any real or perceived security threat, (b) are discriminatory against competitive carriers who must bear increased costs and operational inefficiencies associated with these proposals, and (c) stand in direct contravention of the principles embedded in the Telecommunication Act of 1996 ("Act") mandating physical collocation and efficient use of collocation space.

STATEMENT OF FACTS RELATED TO COVAD OPERATIONS

Covad's views on the current state of collocation security in Massachusetts and Verizon's proposals to radically change the Department's collocation rules are greatly influenced by its actual experience in doing business as a collocated carrier in Massachusetts. Some of the facts related to that experience help to illuminate those views.

A. Covad's Collocation Arrangements in Massachusetts

Generally, Covad has two types of collocation arrangements with Verizon in Massachusetts – caged physical collocation and cageless collocation open environment ("CCOE"). Both arrangements are considered "physical" collocation and provide Covad with necessary, around-the-clock access to its equipment and facilities in the event of routine maintenance and repair, a service outage or other customer emergency. In the past, Covad entered into virtual collocation arrangements with Verizon but, as discussed later, found this method of collocation to be inefficient and unreliable. As a result, Covad currently is converting all virtual collocation arrangements to CCOE. Exh. Covad-1, at 7. Covad's physical collocations include a CCOE arrangement in Hopkinton, which would be converted to virtual if the Department accepts Verizon's recommendation that CCOE be banned where it cannot be provided in separate and secure space (Tr. 546).

B. Covad's Preference for Physical over Virtual Collocation

CCOE arrangements are an attractive alternative to virtual collocation because they are cost- and space-efficient and provide Covad around-the-clock access to equipment and facilities located in the ILEC central office. Unlike virtual collocation arrangements, CCOE arrangements provide Covad direct access to and control over its equipment and facilities for routine maintenance and repair and in the event of a customer emergency. CCOE arrangements also do not require that Covad cede control and ownership of our facilities to Verizon, a major competitor. Exh. Covad-1, at 7.

While there are no technical differences between CCOE arrangements and virtual collocation, virtual collocation presents serious and sometimes insurmountable operational challenges. One such challenge is the management of collocation capacity. Under Verizon's administrative rules, Covad must file an application each time it wants to augment existing

collocation arrangements—a process that usually takes Verizon 76 business days to complete. Thus, every time Covad introduces a new service it must wait 76 business days before the necessary collocation facilities are ready. Even a task as simple as rearranging cards in the DSLAM requires a new collocation application and a corresponding 76 business-day delay before the change takes place. Covad cannot always anticipate a change to customer services that far in advance. This extended processing period for virtual collocation severely strains the optimization of the network and hampers Covad's ability to provide quality service. Exh Covad-1, at 8, Covad Response to Verizon 1-3.

For similar reasons, it is very difficult to manage assets under a virtual collocation arrangement. Once again, any upgrade to the network hardware or firmware is considered a collocation augment, triggering Verizon's 76 business-day application process. Usually, by the time the network upgrade is completed, the installed technology is obsolete, requiring yet another upgrade. Verizon also requires CLECs to supply Verizon with enough maintenance spares for a single collocation arrangement to handle the constant upgrades and repairs to the telecommunications networks. It is not always possible to do this, which causes further delays. Id.

Further, the maintenance services provided to CLEC equipment in a virtual environment are inadequate. While CLECs are required to pay for their own equipment maintenance, the service provided by Verizon is disorganized and generally poor. Verizon experiences significant turnover and reassignment among its technicians, which means that new individuals are constantly being trained at the CLECs' expense. Moreover, in Covad's experience, newly trained technicians often are so poorly trained or simply forget what they have learned that they sometimes require back-up from Covad personnel to complete a task. This is an added expense

as Covad is required to pay both technicians. These higher costs ultimately are borne by the consumer which makes Covad's prices less competitive. Id. at 9.

By converting its existing virtual collocation arrangements to CCOE, Covad will be able to eliminate many of the problems arising from its dependence on Verizon to perform collocation-related services. As with other forms of physical collocation, Covad will be able to: (1) monitor the types of services requested by customers and quickly add to the DSLAM to meet customer demands; (2) make faster upgrades to the network hardware and software; and (3) ensure that reliable, well-trained technicians are always available to maintain its equipment. Despite the obvious benefits, the transition from virtual collocation to CCOE has been unnecessarily delayed by Verizon's own administrative practices. In addition, Covad has been required to make very costly adjustments including: (1) the purchase of additional equipment to collocate in another, secured part of the central office; (2) filing a second collocation application; and (3) awaiting a full collocation interval (76 business days) for site preparation and installation of additional security. These anti-competitive requirements imposed by Verizon have unnecessarily increased the costs associated with collocation as well as resulted in significant delays in completing the transition. Id.

Forcing a change from physical to virtual collocation, as would occur in Hopkinton if the Department adopted Verizon's proposal prohibiting CCOE arrangements, would thus take Covad in the opposite direction from where it would like to go operationally. If that happens Covad would likely leave the Hopkinton CO, and any other CO where it was forced to convert from physical to virtual collocation (Tr. 559). In a virtual arrangement in that CO, Covad would simply be unable to meet the service levels guaranteed in its customer agreements. Id.

ARGUMENT

I. COLLOCATION SECURITY IN MASSACHUSETTS IS GENERALLY WORKING WELL. THE DEPARTMENT SHOULD APPOINT AN INDUSTRY TASK FORCE TO EXAMINE SECURITY ISSUES IN MORE DEPTH AND RECOMMEND CHANGES THAT ADDRESS SPECIFIC DEFICIENCIES IN VERIZON'S SECURITY PRACTICES.

A. The Record Shows that Collocation Security in Massachusetts is Generally Adequate.

While Covad, like all facilities-based telecommunications carriers, remains concerned about potential security threats to its network, the company has not experienced any security breaches in Massachusetts to date. Exh. Covad-1, at 10. Similarly, the Verizon Panel Testimony indicates that Verizon also has not experienced any significant breaches in security in Massachusetts. Exh. VZ-MA-1, at 21. See also Exh. AG-VZ-1-1 and RR-DTE-VZ-3. The fact that two significant carriers in the Massachusetts telecommunications market have had no reports of material incidents involving security breaches or network tampering is a clear indication that the collocation security policies currently in place are adequate and effective. No other carrier reported any network-affecting incidents related to their collocation arrangements in Massachusetts, much less incidents in which their own personnel or the personnel of another CLEC caused damage to Verizon equipment. Indeed, Verizon produced no evidence that a single security breach of any kind had been perpetrated by a CLEC employee or vendor. *See* Verizon Response to RR-DTE-VZ-2.

While Verizon provided no evidence of a network-affecting incident (or any security breach, for that matter) attributable to a CLEC employee or vendor in Massachusetts, it sought to introduce evidence of alleged security breaches in other states, asserting that these incidents are relevant to the current inquiry. Exh. VZ-MA-1, at 22. The Verizon Panel Testimony cites only one specific incident, in Bothel, Washington, in which it claims that a CLEC's actions "caused a

service outage in a remote switch, interrupting service to approximately 9,000 customers." *Id.* at n.9. The incident cited by Verizon, however, involves disputed facts, has yet to be resolved, and Verizon provided no facts regarding the actual security measures in place at the facility in question or any other details about the incident. Exh. Covad-1, at 5-6.[1] This proceeding is too important to be decided on the basis of innuendo, and we urge the Department to focus on experiences that are relevant to collocation operations in Massachusetts.

B. The Department Should Direct Verizon and Other Carriers to Conduct a Thorough Security Review, and Implement Common Sense, Non-Discriminatory, and Cost-Justified Measures to Improve Security.

While there have been no network-affecting incidents involving CLECs in Massachusetts to date, this does not mean the Department should do nothing to improve security in Verizon COs. We believe the Department should support several common sense, non-discriminatory actions. First, before any drastic steps are taken, there should be a more thorough review of existing security issues at Verizon facilities. We believe the Department's immediate focus should be on *examining* security matters rather than hastily requiring changes before all the facts are uncovered. Verizon chose not to supply such facts, relying on generalizations and assertions rather than any data on what is actually occurring in its COs. As such, Covad strongly supports the *Motion* filed in this proceeding on April 25, 2002, recommending that the Department convene an industry task force composed of security personnel from various carriers to examine what security issues or risks actually exist. If the task force concludes that there are actual security risks, the Department should then consider revisions to existing collocation policies.

[1] Moreover, it strains credulity for Verizon to ask the Department to revamp Massachusetts collocation security procedures on the basis of one alleged, unresolved out-of-state incident. If the Department were to evaluate collocation security on a national basis - which it should not and could not do for a whole host of jurisdictional and evidentiary reasons - any such evaluation also would necessarily include consideration of the countless incident-free collocation activities in the fifty states.

To focus the inquiry only on whether CLEC employees should have continued access to Verizon's central offices, however, fails to fully address the larger and more critical security concern. In this regard, through the participation of the industry task force, the Department should expand its inquiry beyond secured access for central offices, as it indicated it would do in the Order. In addition, without necessarily changing its existing collocation policies, the Department could strengthen security measures meant to prevent unauthorized access to all telecommunications networks and infrastructure. This may be accomplished by, among other things, improving personnel training, more comprehensive background checks for CLEC and Verizon employees and vendors, more effective and comprehensive use of "real time" security cameras and alarm monitoring technology, and greater efforts to ensure that only proper personnel/employees have access to the central offices and carrier facilities. Such measures would ensure that only those who should be in central offices can gain access to those facilities and the equipment they house, thereby minimizing the potential for sabotage or terrorist infiltration of Verizon's central offices.

There is evidence in the record that Verizon's security functions and reporting systems would greatly benefit from such a review. For example, when asked about Verizon's security policies and practices with respect to cleaning crews, Verizon's security manager responded that he could not answer the question, as "this is a function of . . . the real estate organization within Verizon. I do not know what their policies are when it comes to this" (Tr. 208). Verizon's Collocation Care Center ("CCC") also lists many incidents as security breaches when they may, in fact, require no attention from the security department itself. *See, e.g.*, Tr. 190 (security deficiencies could include many items, such as burned-out light bulbs, that should be referred to real estate). Verizon security also had no record of an incident report on a router stolen from

Sprint's collocation cage in the Revere central office (Tr. 216).

The measures described above which are designed to strengthen security are non-discriminatory and do not run afoul of the FCC rules and regulations and Department orders that outline the various security measures that may be used by Verizon and other carriers to protect facilities and equipment located in Verizon's central offices. In some cases, Verizon already uses these technologies, only not to the full extent that they could. For example, Verizon has installed CRAS in less than half of its COs, although CRAS can be very useful in tracking the movement of personnel into and out of COs (Tr. 358). Even where CRAS has been installed, Verizon is not using it in ways that could prevent "tailgating," such as using the "swipe out" feature, or using it with still photography to create an accurate visual log of those entering and leaving a facility (Tr. 284, 596).

Verizon also has no consistent policy for the deployment of security guards in COs. The use of guards appears to be driven less by network security concerns than by concerns expressed on an ad hoc basis by personnel in particular buildings. For example, after September 11th, security guards were posted in two additional buildings, but at the request of building managers rather than as a result of a systematic review of security features. Exh. AL-VZ-2-1; Tr. 134-135. Security guards are no longer posted at these locations, but again, Verizon failed to establish that any systematic process resulted in the decision to remove those two guards.

An industry task force would be able to identify these kinds of non-discriminatory measures. Moreover, such an examination of Verizon security practices could weigh the costs associated with any new proposals with the benefits to be achieved by them, something Verizon has not done. Because the costs of any additional security measures inevitably will be borne by CLECs or customers, additional funds spent on security should be spent wisely. Moreover,

proposed measures, especially changes to collocation rules and regulations that would affect CLEC operations, should be narrowly tailored to address real and significant security issues and must be the least expensive, effective alternative available. For example, the Department should explore fully the common sense measures discussed above, which could improve security with no discriminatory impact on CLECs, before considering measures that would have a disproportionate operational and financial impact on CLECs.

Most especially, the Department must ensure that Verizon does not use this proceeding to circumvent existing collocation obligations and increase the CLECs' costs of doing business. These collocation rules and regulations are in place to protect the interests of competitive carriers and ensure the proliferation of facilities-based competition. The security collocation policies in place thus far have proved adequate to protect Verizon's and CLECs' central office facilities from security breaches and harmful attacks. There is no reason to amend these rules absent a compelling security risk, and none has been demonstrated in this proceeding.

II. VERIZON'S PROPOSALS ARE UNWARRANTED, ANTI-COMPETITIVE, AND WOULD VIOLATE THE TELECOMMUNICATIONS ACT OF 1996 AND THE FCC REGULATIONS IMPLEMENTING THE ACT.

Verizon's proposed collocation security plan completely misses the point of the Department's investigation. Rather than offer sound policies designed to minimize security risks introduced by potential terrorist attacks or network tampering, Verizon seeks to advance its long-term agenda of eliminating CLEC access to its central offices altogether. Specifically, Verizon's proposals would: (1) impose a "separate and secure space" rule on all collocation arrangements, requiring existing unsecured CCOE arrangements to be relocated to secure or separated areas of the central office, space permitting, or otherwise converted to virtual collocation; (2) allow virtual collocation only in COs Verizon deems to be "critical" based on unacceptably vague

criteria; (3) establish separate entrances and/or pathways for all forms of physical collocation in order to secure and segregate the collocator's equipment from Verizon's; (4) provide CLECs with reasonable access to shared facilities outside the secured and segregated collocation space only where partitioning of Verizon's equipment is feasible; and (5) provide either virtual collocation and/or escorts for CRTEE arrangements. Verizon completely fails to demonstrate exactly how or why such proposed measures are "appropriate, reasonable and in the public interest," as its witnesses stated in their panel testimony.

The most significant flaw in Verizon's proposal is that it provides no clear rationale for such drastic and anti-competitive changes to rules and regulations that comply with State and Federal law. Verizon proposes one new measure after another, all of which impose unilateral burdens on CLECs, but nowhere does it establish a nexus between its proposals and the security threats the proposals are designed to prevent. Nowhere in its testimony does Verizon identify one threat, real or perceived, that justifies such sweeping changes. To the contrary, Verizon's Panel Testimony spends a significant amount of time identifying *potential* problems that *may* result from a CLEC employees' access to its network premises. No examples of security breaches in Massachusetts are cited and no explanation of how Verizon's proposals solve these *potential* breaches is provided.

The issues now raised by Verizon are the very same claims the FCC and this Department considered in previously rejecting measures similar to those proposed by Verizon in this proceeding. They are some of the same measures rejected by a Federal appeals court on the same day Verizon filed its surrebuttal testimony in this case, offering the same proposals the court rejected in their entirety. *Verizon et al. v. FCC et al*, 292 F.3d 903 (D.C. Cir. 2002). Although the security landscape has changed in the aftermath of the September 11th attacks, the

Department's interest in protecting the integrity of the central offices is the same as before the terrorist attacks. Importantly, the Department's investigation does not suggest that CLECs pose a national security threat, making Verizon's narrow focus on limiting CLEC access even more difficult to justify. Unless and until Verizon puts forth a compelling explanation for its proposals that is related in some way to security concerns that have only come to light after September 11th, such as the risk of terrorist infiltration, they must be rejected.

A. Verizon's Proposal to Segregate CLEC Equipment From Its Own Would Provide No Tangible Security Benefits While Substantially Affecting CLECs' Ability to Do Business in Massachusetts.

Verizon's proposal to impose a blanket "separate and secure space only" requirement on physical collocation, including CCOE arrangements, has three strikes going against it. First, the proposal contravenes the FCC's collocation regulations that were promulgated in *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, CC Docket No. 98-147, Fourth Report and Order, FCC 01-204 (August 8, 2001)("*Collocation Remand Order*"). These regulations were upheld by the D.C. Circuit on June 18, 2002. *Verizon et al. v. FCC et al*, 292 F.3d 903 (D.C. Cir. 2002). There is simply no way to reconcile this proposal with the current state of the law. Verizon recognized this fact in its pre-filed testimony, which suggested that the Department petition the FCC to change its regulations to allow Verizon to impose its anti-competitive rules on Massachusetts CLECs. The Department should reject the "separate and secure space only" proposal as unlawful, and should decline Verizon's invitation to ask the FCC to substitute a well-balanced and competitively neutral rule for one that would, in Covad's case, make doing business in some Massachusetts COs impossible.

The second strike against this proposal is its extraordinary impact on CLECs, including Covad. Verizon continually downplayed the effect of this proposal, stating that only one CCOE

arrangement would have to be moved. As discussed in the Statement of Facts, this CCOE arrangement, in the Hopkinton CO, belongs to Covad, and the proposal to convert it to virtual is hardly benign. In fact, because virtual collocation is so operationally inferior to physical, Covad would be unable to continue to serve its customers in the Hopkinton CO if its CCOE were converted to virtual. Without a physical collocation arrangement there, Covad would abandon the Hopkinton CO (Tr. 559).

While the impact on Covad's business from this proposal would be immediate, the long-term impact, which Verizon ignores completely, would be significant as well. The proposal would ban the use of CCOE where CLEC and ILEC equipment would be "commingled." Of course, this is one of the attractive characteristics of CCOE, that it allows for physical collocation in COs that might otherwise be exhausted for physical collocation. This proposal, by definition, would result in earlier CO exhaust, especially since CCOE arrangements have already been placed in separate and secure space in some COs, rather than commingled with Verizon equipment. Verizon's argument that this will not matter because the demand for physical collocation seems to be dropping is cynical in the extreme. Verizon is saying, in effect, that the Department should not worry about accommodating greater future demand for collocation arrangements because Verizon is counting on its competition getting weaker rather than stronger. If the Department adopts this type of reasoning, that argument will become a self-fulfilling prophecy.

The third strike against this proposal is that it is unsupported by any evidence that it would result in better security in COs. This is due in part to the fact that Verizon simply fails to understand that on the issue of network security all carriers are on the same side. No carrier wants to risk the security and integrity of its network to acts of terror or vandalism by third

parties. Consequently, any efforts to truly deter such activity must result from a cooperative effort of all parties involved.

Verizon presents no evidence to the contrary that would allow the Department to conclude that CLECs pose a risk to its equipment and facilities. CCOE arrangements do not present an added security risk just because they are located in an area where other Verizon equipment is located. CLECs have every reason to ensure the integrity of the Verizon network. CLEC technicians, the apparent source of Verizon's security concerns, are subject to background checks by both their CLEC employers *and* Verizon. While we know there are no guarantees, this practice is probably the most reliable way for CLECs and Verizon to detect potential terrorists in the ranks.

In Covad's experience, CCOE arrangements actually provide higher levels of security from tampering and terrorists activities, as the foot traffic in the central office is likely to be greater than with other collocation arrangements. With more people around from different companies, it is highly unlikely that any carrier's employee will tamper with another carrier's equipment for fear of being caught and subsequent reprisal. Further, Verizon's assertion that CLEC employees might work on the wrong shelf or equipment is unfounded. There is no evidence of such a problem occurring in Massachusetts, and to the extent there is even a chance of this happening, that chance could be reduced by reviewing and, if necessary, improving Verizon's equipment identification methods.

B. Verizon's "Critical CO" Proposal Would Violate the Act, and Reduce Competition without Any Demonstrable Increase in Security.

The "critical CO" proposal is the strongest manifestation of Verizon's unswerving desire to eliminate access by CLEC personnel to its central offices. Having failed in all of its other attempts to accomplish this goal, Verizon would now exploit the tragedy of September 11th for

yet another bite at this apple. The current argument is that some COs (we do not know which ones) are simply too important (not necessarily too vulnerable, since we cannot know anything about the actual security status at any of these unidentified facilities) because of certain characteristics (we do not know which characteristics) to allow anyone other than a Verizon employee or vendor (or visitor) to enter.

This proposal clearly contravenes the requirements of the Act and Massachusetts law. Use of physical collocation is not merely some inconvenient option, as Verizon suggests. Rather, the strong preference for physical collocation is embedded in the Act, which requires ILECs to "provide, on rates, terms and conditions that are just, reasonable and nondiscriminatory, for physical collocation of equipment . . . at the premises of the local exchange carrier[.]" 47 U.S.C. 251(c)(6). This has been further borne out by the overwhelming majority of CLECs who prefer physical collocation over other alternatives so as to maximize control and efficiency over their own networks, thereby reducing costs to consumers. The only exception to this rule is where technical and space limitations prevent physical collocation. Verizon does not even offer a legal argument that its "critical CO" proposal is based on this "technically infeasible" exception. This is not surprising, since the criteria suggested by Verizon focus on the customers the facility serves or the type of equipment located in the facility, rather than Verizon's technical ability to accommodate CLECs. Thus, even assuming, *arguendo*, that virtual collocation reduces the possibility of a terrorist threat at all (a dubious proposition), the elimination of physical collocation would require more than a petition to the FCC; it would require a statutory amendment by Congress. Without such a change in the Act itself, this

proposal must be rejected.[2]

As with the "separate and secure space only" proposal, there is also no evidence of any real benefits that would be gained from the "critical CO" measure in exchange for the tremendous damage it would do to competition in Massachusetts. As discussed above, there is no evidence that CLEC personnel pose any threat that is different or greater than the threat posed by Verizon personnel. Verizon's actual experience in Massachusetts bears this out. There have been no outages whatsoever, or serious security breaches of any kind, for that matter, attributable to the presence of CLEC personnel in COs. *See* Exh. VZ-MA-1, at 21; Verizon Responses to RR-DTE-VZ-2. On the other side of the ledger, every single CLEC that appeared in this case focused on the operational inferiority of virtual collocation, and the severe impact on their ability to serve customers if any of their physical arrangements must be converted to virtual. Verizon dismisses these concerns, but their dismissal lacks credibility. None of the Verizon witnesses has ever worked for a CLEC. None of them has any experience trying to deal with Verizon in gaining access to CO space that is critical for a company providing facilities-based services. The Department should not ignore the collective experience of the CLEC community in Massachusetts, especially where the vague criteria for choosing "critical" COs is likely to identify facilities that are as critical to CLECs as they are to Verizon.

C. Verizon's Proposal to Require Separate Entrances and/or Pathways for All Forms of Physical Collocation Would Not Be an Effective Means of Securing Carriers' Networks and Equipment.

Requiring separate space and entrances for physical collocation arrangements would

[2] In a last-minute attempt to make its "critical CO" proposal seem something other than blatantly discriminatory, Verizon witnesses testified that, if the Department adopts this proposal, Verizon would also exclude non-employee cleaning crews at COs where CLECs personnel had been banned (Tr. 139, 338). This suggestion is a ruse, and a rather transparent one. If Verizon believed non-employee cleaning crews constituted a threat to network security, it could have excluded them from any or all COs long ago.

provide no tangible security benefits for the Massachusetts telecommunications infrastructure. Again, the CLEC employees are not the concern here. All facilities-based carriers share the same concerns and interests in ensuring the safety and integrity of the telecommunications infrastructure. Verizon's Panel Testimony suggests that isolating Verizon's equipment from CLEC employees will somehow discourage terrorist sabotage. Exh. VZ-MA-1, at 23, 28. There is no evidence to support this claim. To the contrary, the addition of more entrances and egresses only adds to the security risks as it increases individual access to the building. Moreover, the construction of separate entrances does little to protect the CLECs' facilities because even in a separate environment, Verizon's maintenance crew would still have access to such premises.

In addition, Verizon fails to demonstrate that separate entrances in this instance would be permitted under the FCC's rules. Pursuant to Section 51.323(i)(6) of FCC's rules, the ILECs may not construct or require construction of separate entrances unless the following conditions are met: (1) construction of a separate entrance is technically feasible; (2) legitimate security concerns exist; (3) construction of a separate entrance will not automatically delay collocation provisioning; and (4) construction of a separate entrance will not materially increase the requesting carrier's costs. 47 C.F.R. 51.323(i)(6). While it is probably technically feasible to construct separate entrances, the costs of doing so would undoubtedly increase CLEC expenses and delay collocation provisioning, which is inconsistent with the FCC's rules. The D.C. Circuit's decision in *Verizon et al. v. FCC et al.* upheld the FCC's rejection of a blanket separate entrance requirement.

Likewise, Verizon has not clearly identified any security concerns that would warrant the construction of separate entrances. The security concerns raised by Verizon again all point to the

potential for CLEC tampering with ILEC equipment located in the central office, concerns that have not been borne out to date. Indeed, these concerns were considered and eventually dismissed by the FCC in promulgating its collocation rules.

D. Verizon's Proposal to Eliminate Access to Common Areas Where Separate Barriers Cannot Be Erected Around Verizon Equipment Is Unnecessary.

Verizon's proposal seeks to provide access to such facilities only where convenient. Access to shared facilities, however, is not an "optional" service as Verizon suggests. Rather, Verizon is required to provide access to common areas such as restrooms, loading docks and elevators by FCC and OSHA regulations and must continue do so even when it cannot separate or secure its equipment from common areas. Moreover, Covad disagrees with Verizon's assertion that escorts are needed to accompany CLEC employees and vendors accessing shared facilities, at least to the extent CLECs would be required to absorb the costs. As this Department and the FCC have determined in the past, it is an unnecessary measure that only increases the need for additional manpower and drives up the cost of doing business. Exh. Covad-1, at 19-20.

E. Verizon's Proposal that the Department Not Require Physical Collocation at Remote Terminal Equipment Enclosures is Premature.

Verizon's concerns regarding remote terminal equipment enclosures ("RTEEs") are premature since, as Verizon admits, there currently are no RTEE arrangements in Massachusetts. Once again, Verizon seeks to have the Department impose more restrictive security measures on CLECs even where there is no evidence of a security risk. Absent its speculative analysis, Verizon fails to adequately explain the potential security risks that exist from physical collocation arrangements in RTs. As far as Covad can tell, Verizon appears to think the size of RTs present the most serious consideration. If RTs are a security risk due to their small size, perhaps Verizon should reconsider whether they should be used at all. In the final analysis,

security at RTs should be handled no differently than at central offices, with the same rights of access and collocation. Exh. Covad-1, at 19.

Conclusion

In this proceeding, while the Department sought an open and honest examination of security of Verizon facilities in Massachusetts, Verizon itself responded only with a series of proposals that would drastically re-write the rules for collocating CLECs. Verizon provided neither evidence to support the basic assumptions that underlay these proposals (such as the idea that CLECs do not have the same interest as Verizon in protecting the network), nor evidence that the measures would enhance security whatsoever. Covad asks that the Department reject these anti-competitive proposals and, in their place, order the formation of an industry task force that would evaluate the status of collocation security measures, and, if warranted, recommend sensible, non-discriminatory, and cost-effective improvements to those measures.

Respectfully submitted,

COVAD COMMUNICATIONS COMPANY
By its attorneys

_____

Robert D. Shapiro
Christopher H. Kallaher
Rubin and Rudman LLP
50 Rowes Wharf
Boston, MA 02110
Tel. No. (617) 330-7000

_____

Tony Hansel
Covad Communications Company
Hamilton Square
600 14th Street NW, Suite 750
Washington, DC 20005

Dated: August 9, 2002